Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method of generating a password for use by an end-user device (UE) to access a remote server, comprising:

sending a request for access from the UE to the remote server;

creating a temporary identity for the UE by said remote server;

sending to an authentication node in the UE's home network details of the request for access, said details including said temporary identity for the UE;

at the authentication node or the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge to said UE using an algorithm capable of generating end-user password, including details of the temporary identity of the UE and identity of said remote server;

at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the identity of the UE;

storing the password and the temporary identity of the UE at the UE; and

sending an authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server.

2. (Previously Presented) The method in claim 1, wherein the algorithm capable of generating end-user passwords is HTIP Digest Authentication and Key Agreement (AKA).

3. (Previously Presented) The method in claim 1, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating

the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE.

4. (Cancelled)

5. (Previously Presented) The method in claim 1, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node.

6. (Previously Presented) The method in claim 5, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE.

7. (Previously Presented) The method in claim 5, wherein the password is stored at the authentication node.

8. (Previously Presented) The method in claim 5, further comprising authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the password has been generated.

9. (Previously Presented) The method in claim 1, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly.

10. ((Previously Presented) The method in claim 9, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server.

11. (Previously Presented) The method in claim 9, wherein the HTTP Digest Challenge is generated at the remote server.

12. (Previously Presented) The method in claim 10, further comprising sending the HTTP digest challenge from the remote server to the UE.

13. (Previously Presented) The method in claim 11, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server.

14. (Previously Presented) The method in claim 9, further comprising authenticating the UE at the authentication node and returning an authentication result to the remote server.

15. (Cancelled)

16. (Previously Presented) The method in claim 11, further comprising sending an authentication request from the remote server to the authentication node, sending the password from the authentication node to the remote server, and authenticating the UE at the remote server.

17. (Previously Presented) The method in claim 1, further comprising sending an authentication request from the remote server to the authentication node authenticating the UE at the authentication node, and sending confirmation of authentication from the authentication node to the remote server.

18. (Previously Presented) A method of authentication an end-user device (UE) with a remote server, comprising the steps of:

receiving a request for access from said UE by said remote server;

creating the temporary identity for the UE_by said remote server;

sending to an authentication node in the UE's home network details of the request for access, said details including said temporary identity created by said remote server and instructing said authentication node to generate a Hypertext Transfer Protocol (HTTP) Digest challenge using an algorithm capable of generating end-user password with said details;

at the UE, generating a password based on the HTIP Digest challenge, said password being associated with the temporary identity of the UE created by said remote server;

storing the password and the temporary identity of the UE at the UE; and

receiving a first authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server.

19. (Previously Presented) The method in claim 18, wherein the algorithm capable of generating end-user passwords is HTTP Digest Authentication and Key Agreement (AKA).

20. (Previously Presented) The method in claim 18, further comprising sending the identity of the remote server to the authentication node, wherein the step of generating the HTTP Digest challenge includes using the identity of the remote server, and wherein the identity of the remote server is stored at the UE.

21. (Cancelled)

22. (Previously Presented) The method in claim 18, wherein the step of sending details of the request for access to the authentication node includes redirecting the request for access to the authentication node.

23. (Previously Presented) The method in claim 18, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node directly to the UE.

24. (Previously Presented) The method in claim 23, wherein the password is stored at the authentication node.

25. (Previously Presented) The method in claim 23, further comprising authenticating the UE at the authentication node and redirecting the request for access from the authentication node to the remote server after the password has been generated.

26. (Previously Presented) The method in claim 18, wherein the step of sending details of the request for access to the authentication node includes the remote server contacting the authentication node directly.

27. (Previously Presented) The method in claim 26, wherein the HTTP Digest challenge is generated at the authentication node and sent from the authentication node to the remote server.

28. (Previously Presented) The method in claim 26, wherein the HTTP Digest challenge is generated at the remote server.

29. (Previously Presented) The method in claim 28, further comprising sending the HTTP digest challenge from the remote server to the UE.

30. (Previously Presented) The method in claim 29, further comprising including a HTTP Digest AKA challenge password in the information sent from the authentication node to the remote server and authenticating the UE at the remote server.

31. (Previously Presented) The method in claim 28, further comprising authenticating the UE at the authentication node and returning an authentication result to the remote server.

32. (Previously Presented) The method of claim 1, further comprising the steps of:

receiving a subsequent request for access from the UE to the remote server;

at the remote server, generating a second Hypertext Transfer Protocol (HTTP) Digest challenge including details of the identity of the remote server and sending the challenge to the UE; and

at the UE, sending a second authentication response including said temporary identity of the UE and a proof of possession of the password to the remote server and performing said authentication without generating any additional password and without contacting said authentication node in the home network.

33. (Previously Presented) The method of claim 18, further comprising the steps of:

receiving a second request for access from the UE to the remote server;

at the remote server, generating a second Hypertext Transfer Protocol (HTTP) Digest challenge including details of the identity of the remote server and sending the challenge to the UE; and

receiving a second authentication response from said UE including said temporary identity of the UE and a proof of possession of the password thereby performing said authentication without generating any additional password and without contacting said authentication node in the home network.

* * *